

The Černý conjecture for one-cluster automata with prime length cycle

Benjamin Steinberg*

School of Mathematics and Statistics
Carleton University
1125 Colonel By Drive
Ottawa, ON, Canada
bsteinbg@math.carleton.ca

Abstract. We prove the Černý conjecture for one-cluster automata with prime length cycle. Consequences are given for the hybrid Road-coloring-Černý conjecture for digraphs with a proper cycle of prime length.

1 Introduction

Let $\mathcal{A} = (Q, \Sigma)$ be a finite (deterministic) automaton with state set Q and input alphabet Σ . A word $w \in \Sigma^*$ is called a *reset word* for \mathcal{A} if it brings all states to a single state, that is, $|Qw| = 1$. An automaton admitting a reset word is said to be *synchronizing*. The following conjecture is due to Černý.

Conjecture 1 (Černý [29]). *An n -state synchronizing automaton admits a synchronizing word of length at most $(n - 1)^2$.*

The literature on this subject is constantly growing, cf. [1–7, 9–14, 16, 17, 19–27, 29, 30]. The best known upper bound is $(n - 1)^3/6$ [18], whereas it is known that one cannot do better than $(n - 1)^2$ [29].

Béal and Perrin [8, 9] defined an automaton $\mathcal{A} = (Q, \Sigma)$ to be a *one-cluster automaton* if there exists $a \in \Sigma$ such that a has only one cycle on Q . More precisely, this means that the graph obtained by considering only the edges labeled by a is connected. We shall always denote the a -cycle by C ; see Figure 1. The level ℓ of \mathcal{A} is the least non-negative integer such that $Qa^\ell \subseteq C$. Of course, $\ell \leq |Q| - |C|$. If the letter a is not clear from context, then we say that \mathcal{A} is one-cluster with respect to a .

A one-cluster automaton of level 0, i.e., one in which $Q = C$, is called a *circular automaton*. The Černý conjecture was solved by Pin [16] for

* The author gratefully acknowledges the support of NSERC. Version of May 11, 2010.

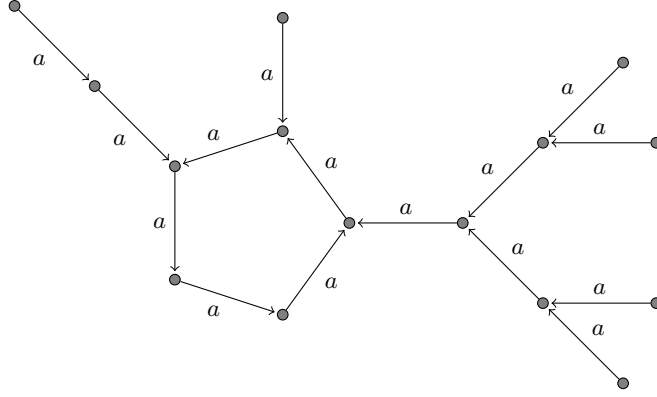


Fig. 1. a -skeleton of a one-cluster automaton with $|Q| = 15$ and $|C| = 5$.

circular automata with a prime number of states and by Dubuc [12] in the general case (20 years later). We prove here that the Černý conjecture is true for one-cluster automata with prime length cycle, generalizing Pin's result. It is our hope to adapt the techniques of Dubuc [12] to handle the general case in a later paper.

We also consider the hybrid Road Coloring-Černý problem, introduced by Volkov. A strongly connected digraph is said to be *aperiodic* if the greatest common divisor of its cycle lengths is one. If Γ is any strongly connected aperiodic digraph with constant out-degree $|\Sigma|$, then by Trahtman's Road Coloring theorem [28] there is a way to label the edges of Γ by Σ , i.e., to color Γ , in order to obtain a synchronizing automaton (Q, Σ) . The hybrid question is to find the minimum length of a reset word over all possible synchronizing colorings. As a consequence of our main result, we show that any strongly connected aperiodic digraph with constant out-degree and no multiple edges containing a proper prime length cycle admits a synchronizing coloring with a reset word of length at most $(n - 1)^2$ where n is the number of vertices.

2 Proof of the main result

Fix for this section a one-cluster synchronizing automaton $\mathcal{A} = (Q, \Sigma)$ with n states, level ℓ and cycle C of prime length p with respect to the letter a . Without loss of generality, we may take $Q = \{1, \dots, n\}$. Denote

by $\pi: \Sigma^* \rightarrow M_n(\mathbb{Q})$ the matrix representation associated to \mathcal{A} ; so

$$\pi(w)_{q,r} = \begin{cases} 1 & qw = r \\ 0 & \text{else.} \end{cases}$$

If $S \subseteq Q$, then $[S]$ denotes the characteristic row vector of S . Denote by v^T the transpose of a row vector v . Usually, we omit π from the notation and write things like $[S]w$ or $w[S]^T$. Note that $w[S]^T = [Sw^{-1}]^T$ where $Sw^{-1} = \{q \in Q \mid qw \in S\}$. If $S \subseteq Q$, let

$$\gamma_S = [S]^T - (|S|/p)[Q]^T$$

and observe that

$$w\gamma_S = [Sw^{-1}]^T - (|S|/p)[Q]^T$$

for any $w \in \Sigma^*$. Also we have

$$[C]w\gamma_S = |C \cap Sw^{-1}| - |S| \tag{1}$$

for $w \in \Sigma^*$.

If $V \subseteq \mathbb{Q}^n$ is a subspace of column vectors, then Σ^*V denotes the smallest subspace containing V and invariant under Σ^* . If V is spanned by v_1, \dots, v_r , then Σ^*V is spanned by the elements wv_i with $w \in \Sigma^*$. The following lemma is a standard ascending chain argument: see for example [14, 24, 25] for a proof.

Lemma 2. *Let $\pi: \Sigma^* \rightarrow M_n(\mathbb{Q})$ be a representation and let $W \subseteq V$ be subspaces of \mathbb{Q}^n consisting of column vectors such that $\Sigma^*W \not\subseteq V$. Let A be a spanning set for W . Then there exist $w \in \Sigma^*$ and $a \in A$ such that $wa \notin V$ and $|w| \leq \dim V - \dim W + 1$.*

The next proposition characterizes the fixed column vectors of a . By an a -path in \mathcal{A} , we mean a path all of whose edges have label a .

Proposition 3. *Let $v \in \mathbb{Q}^n$ be a column vector such that $av = v$. Then $v = k[Q]^T$ for some $k \in \mathbb{Q}$.*

Proof. Routine computation shows that for any state q , one has $(av)_q = v_{qa}$. Thus if $av = v$, then $v_q = v_{qa}$ for any $q \in Q$. Hence, by iteration, if there is an a -path from q to q' , then $v_q = v_{q'}$. But if q_0 belongs to the cycle C , then every state has an a -path to q_0 . Thus, all entries of v are the same rational number k , that is, $v = k[Q]^T$.

Our next lemma is crucial in taking advantage of the prime cycle length.

Lemma 4. *Suppose $\emptyset \neq S \subsetneq C$ and let $A = \{a^{\ell+j}\gamma_S \mid 0 \leq j \leq p-1\}$. Let W be the span of A . Then we have: the subspace W is invariant under $\pi(a)$, the minimal polynomial of $\pi(a)$ on W is the cyclotomic polynomial $1 + x + x^2 + \cdots + x^{p-1}$ and $\dim W = p - 1$.*

Proof. Clearly a^ℓ and $a^{\ell+p}$ act the same on Q and so $\pi(a)^\ell = \pi(a)^{\ell+p}$. It follows that W is invariant under $\pi(a)$, and $\pi(a)^p$ acts on W as the identity. Therefore, the minimal polynomial $m(x)$ of $\pi(a)$ on W divides $x^p - 1$. Next observe that W is contained in $[C]^\perp$ since the fact that a permutes the states of C implies $[C]a^{\ell+j}\gamma_S = [C]\gamma_S = 0$. Thus W does not contain any non-zero multiple of $[Q]^T$. It follows from Proposition 3 that 1 is not an eigenvalue of the restriction of $\pi(a)$ to W . Since p is prime, the factorization over \mathbb{Q} of $x^p - 1$ into irreducibles is $(x-1)(1+x+\cdots+x^{p-1})$. We conclude that $m(x) = 1+x+\cdots+x^{p-1}$. In particular, $\dim W \geq p-1$. Also, $m(\pi(a))a^\ell\gamma_S = 0$ implies that $a^{\ell+p-1}\gamma_S = -\sum_{j=0}^{p-2} a^{\ell+j}\gamma_S$ and so W is spanned by $p-1$ elements. Thus $\dim W = p-1$.

We need to bound from below the dimension of another subspace.

Proposition 5. *Let $W = \text{Span}\{a^\ell\gamma_q \mid q \in C\}$. Then $\dim W \geq p-1$.*

Proof. Let $C = \{q_1, \dots, q_p\}$ and define a vector space morphism $\mathbb{Q}^n \rightarrow \mathbb{Q}^p$ by $[q_i]^T \mapsto e_i$ and $[q]^T \mapsto 0$ for $q \notin C$, where e_i is the i^{th} standard unit vector. Then the image of W is the space spanned by the vectors $e_j - (1/p)(e_1 + \cdots + e_p)$ with $1 \leq j \leq p$. But these vectors form a basis for the orthogonal complement of $e_1 + \cdots + e_p$. It follows $\dim W \geq p-1$.

Our last lemma relies on Lemma 2.

Lemma 6. *Let $\emptyset \neq S_1, \dots, S_k \subsetneq C$ and $w_1, \dots, w_k \in \Sigma^*$. Put $W = \text{Span}\{w_i\gamma_{S_i} \mid 1 \leq i \leq k\}$. Suppose that*

$$\sum_{i=1}^k w_i\gamma_{S_i} = 0.$$

Then there exist $w \in \Sigma^$ and $1 \leq j \leq k$ such that $|C \cap S_j w_j^{-1} w^{-1}| > |S_j|$ and $|w| \leq n - \dim W$.*

Proof. First we claim that there exist $w \in \Sigma^*$ and $1 \leq t \leq k$ with $|w| \leq n - \dim W$ and $|C \cap S_t w_t^{-1} w^{-1}| - |S_t| \neq 0$. By (1), this amounts to finding w of length at most $n - \dim W$ and $1 \leq t \leq k$ with $ww_t \gamma_{S_t} \notin [C]^\perp$. In particular, we are done if $W \not\subseteq [C]^\perp$. So assume $W \subseteq [C]^\perp$. In particular, $0 = [C]w_1 \gamma_{S_1} = |C \cap S_1 w_1^{-1}| - |S_1|$ and so $C \cap S_1 w_1^{-1} \neq \emptyset$. Let u be a reset word. Since $C = Qa^\ell a^*$, we may assume that u resets to a state in $C \cap S_1 w_1^{-1}$. Then

$$[C]uw_1 \gamma_{S_1} = |C \cap S_1 w_1^{-1} u^{-1}| - |S_1| = |C| - |S_1| \neq 0.$$

It follows $\Sigma^* W \not\subseteq [C]^\perp$ and so by Lemma 2 we can find $w \in \Sigma^*$ and $1 \leq t \leq k$ with $ww_t \gamma_{S_t} \notin [C]^\perp$ and $|w| \leq \dim[C]^\perp - \dim W + 1 = n - \dim W$.

Next observe that

$$\sum_{i=1}^k (|C \cap S_i w_i^{-1} w^{-1}| - |S_i|) = \sum_{i=1}^k [C]w w_i \gamma_{S_i} = [C]w \sum_{i=1}^k w_i \gamma_{S_i} = 0.$$

Since the term $|C \cap S_t w_t^{-1} w^{-1}| - |S_t| \neq 0$, there must exist $1 \leq j \leq k$ such that $|C \cap S_j w_j^{-1} w^{-1}| - |S_j| > 0$, that is, $|C \cap S_j w_j^{-1} w^{-1}| > |S_j|$. This completes the proof.

Our final proposition before proving the main result is a simple computation with derivatives.

Proposition 7. *Let $n > 0$ be a fixed integer. Then the function*

$$f(t) = 3n - 3t + 1 + (t - 2)(2n - t)$$

is bounded by $(n - 1)^2$ on the interval $[1, n - 1]$.

Proof. We compute $f'(t) = -3 + 2n - t - t + 2 = 2n - 1 - 2t$ and so is positive for $t < n - \frac{1}{2}$. Thus f is increasing on the interval $[1, n - 1]$ and hence takes its maximum value at $t = n - 1$. Substituting in, we obtain $f(t) \leq 3n - 3(n - 1) + 1 + (n - 3)(n + 1) = 4 + n^2 - 2n - 3 = n^2 - 2n + 1 = (n - 1)^2$.

We can now prove the main result.

Theorem 8. *Let $\mathcal{A} = (Q, A)$ be a synchronizing one-cluster automaton with n states, level ℓ and cycle C of prime length p . Then \mathcal{A} has a reset word of length at most*

$$n - p + 1 + 2\ell + (p - 2)(n + \ell)$$

which is bounded above by $(n - 1)^2$.

Proof. Assume \mathcal{A} is one-cluster with respect to the letter a . We maintain the above notation. The proof rests on two claims.

Claim 1. Let $S \subseteq C$ with $2 \leq |S| < p$. Then there exists a word $w \in \Sigma^*$ such that $|C \cap Sw^{-1}| > |S|$ and $|w| \leq n + \ell$.

Proof (of claim). Let $W = \text{Span}\{a^{\ell+j}\gamma_S \mid 0 \leq j \leq p-1\}$. Then $\dim W = p-1$ and the minimal polynomial of $\pi(a)$ on W is $m(x) = 1+x+\dots+x^{p-1}$ by Lemma 4. Also,

$$\sum_{0 \leq j \leq p-1} a^{\ell+j}\gamma_S = m(\pi(a))a^\ell\gamma_S = 0$$

because $a^\ell\gamma_S \in W$. Lemma 6 now implies we can find v of length at most $n - \dim W = n - (p-1)$ and $0 \leq j \leq p-1$ such that

$$|C \cap S(a^{\ell+j})^{-1}v^{-1}| > |S|.$$

Taking $w = va^{\ell+j}$ does the job because $|w| \leq n - (p-1) + \ell + p - 1 \leq n + \ell$.

Our next claim deals with the case $|S| = 1$.

Claim 2. There exists $q \in C$ and a word w of length at most $n - p + 1 + \ell$ such that $|C \cap qw^{-1}| > 1$.

Proof (of claim). Let $W = \text{Span}\{a^\ell\gamma_q \mid q \in C\}$. Then $\dim W \geq p-1$ by Proposition 5. Next observe that

$$\begin{aligned} \sum_{q \in C} a^\ell\gamma_q &= a^\ell \sum_{q \in C} ([q]^T - (1/p)[Q]^T) = a^\ell([C]^T - [Q]^T) \\ &= [C(a^\ell)^{-1}]^T - [Q]^T = [Q]^T - [Q]^T = 0 \end{aligned}$$

where the penultimate equality uses that $Qa^\ell = C$. Lemma 6 now provides $q \in C$ and $u \in \Sigma^*$ with $|C \cap q(a^\ell)^{-1}u^{-1}| > 1$ and $|u| \leq n - \dim W \leq n - p + 1$. Taking $w = ua^\ell$ proves the claim.

To complete the proof first observe that, by Claim 2, we can find a state $q \in C$ and a word w_0 of length at most $n - p + 1 + \ell$ such that $|C \cap qw_0^{-1}| > 1$. Then applying Claim 1, we can find a word w_1 of length at most $n + \ell$ such that

$$|C \cap qw_0^{-1}w_1^{-1}| \geq |C \cap (C \cap qw_0^{-1})w_1^{-1}| > |C \cap qw_0^{-1}|.$$

Continuing in this fashion we can find words w_1, \dots, w_k of length at most $n + \ell$, where $k \leq p-2$, such that $|C \cap qw_0^{-1}w_1^{-1} \dots w_k^{-1}| = |C|$, i.e.,

$C \subseteq q(w_k \cdots w_0)^{-1}$. Then $Qa^\ell w_k \cdots w_1 w_0 = Cw_k \cdots w_0 = \{q\}$ and so we have found a reset word $w = a^\ell w_k \cdots w_1 w_0$ of length at most

$$n - p + 1 + 2\ell + (p - 2)(n + \ell).$$

Next, using that $\ell \leq n - p$, we obtain an upper bound on $|w|$ of $3n - 3p + 1 + (p - 2)(2n - p)$. If $p = n$, then the upper bound becomes $1 + (n - 2)n = (n - 1)^2$. If $p \leq n - 1$, Proposition 7 yields $|w| \leq (n - 1)^2$, as required.

It was observed in [11] that a bound on synchronizing one-cluster automata with prime length cycle leads to bounds for the hybrid Road Coloring-Černý conjecture.

Corollary 9. *Let Γ be a strongly connected aperiodic digraph with constant out-degree, n vertices and no multiple edges. Suppose moreover that Γ contains a cycle of prime length $p < n$. Then Γ admits a synchronizing word of length at most $3n - 3p + 1 + (p - 2)(2n - p) \leq (n - 1)^2$.*

Proof. Let C be the cycle of length p . A result of O'Brien [11, 15] implies that Γ admits a synchronizing coloring that turns it into a one-cluster automaton with C as the cycle. The result now follows from Theorem 8.

Remark 10. Note that Lemma 5 does not rely on the cycle having prime length. Using the proof scheme of Theorem 8 and the ideas of [24], one can show that if \mathcal{A} is a one-cluster automaton with n states, level ℓ and cycle length n , then there is an upper bound of $n - m + 2 + 2\ell + (m - 2)(2n - 3)$ on the length of a reset word. Using that $\ell \leq n - m$ yields an upper bound of $3n - 3m + 2 + (m - 2)(2n - 3) = m(2n - 6) - n + 8$. Assuming $m < n$ (since the case $m = n$ is handled by [12]), gives an upper bound of $(n - 1)(2n - 6) - n + 8 = 2n^2 - 9n + 14$.

Acknowledgments

Steffen Kopecki produced the diagram in Figure 1.

References

1. J. Almeida, S. Margolis, B. Steinberg, and M. Volkov. Representation theory of finite semigroups, semigroup radicals and formal language theory. *Trans. Amer. Math. Soc.*, 361(3):1429–1461, 2009.

2. J. Almeida and B. Steinberg. Matrix mortality and the Černý-Pin conjecture. In *Developments in language theory*, volume 5583 of *Lecture Notes in Comput. Sci.*, pages 67–80. Springer, Berlin, 2009.
3. D. S. Ananichev and M. V. Volkov. Some results on Černý type problems for transformation semigroups. In *Semigroups and languages*, pages 23–42. World Sci. Publ., River Edge, NJ, 2004.
4. D. S. Ananichev and M. V. Volkov. Synchronizing generalized monotonic automata. *Theoret. Comput. Sci.*, 330(1):3–13, 2005.
5. D. S. Ananichev, M. V. Volkov, and Y. I. Zaks. Synchronizing automata with a letter of deficiency 2. *Theoret. Comput. Sci.*, 376(1-2):30–41, 2007.
6. F. Arnold and B. Steinberg. Synchronizing groups and automata. *Theoret. Comput. Sci.*, 359(1-3):101–110, 2006.
7. M.-P. Béal. A note on Cerny’s conjecture and rational series. Unpublished, 2003.
8. M.-P. Béal, M. V. Berlinkov, and D. Perrin. A quadratic upper bound on the size of a synchronizing word in one-cluster automata. *International Journal of Foundations of Computer Science*, To appear.
9. M.-P. Béal and D. Perrin. A quadratic upper bound on the size of a synchronizing word in one-cluster automata. In *Developments in language theory*, volume 5583 of *Lecture Notes in Comput. Sci.*, pages 81–90. Springer, Berlin, 2009.
10. A. Carpi and F. d’Alessandro. The synchronization problem for strongly transitive automata. In *Developments in language theory*, volume 5257 of *Lecture Notes in Comput. Sci.*, pages 240–251. Springer, Berlin, 2008.
11. A. Carpi and F. d’Alessandro. The synchronization problem for locally strongly transitive automata. In *Mathematical Foundations of Computer Science*, volume 5734 of *Lecture Notes in Comput. Sci.*, pages 211–222. Springer, Berlin, 2009.
12. L. Dubuc. Sur les automates circulaires et la conjecture de Černý. *RAIRO Inform. Théor. Appl.*, 32(1-3):21–34, 1998.
13. J. Kari. A counter example to a conjecture concerning synchronizing words in finite automata. *Bull. Eur. Assoc. Theor. Comput. Sci. EATCS*, (73):146, 2001.
14. J. Kari. Synchronizing finite automata on Eulerian digraphs. *Theoret. Comput. Sci.*, 295(1-3):223–232, 2003. Mathematical foundations of computer science (Mariánské Lázně, 2001).
15. G. L. O’Brien. The road-colouring problem. *Israel J. Math.*, 39(1-2):145–154, 1981.
16. J.-E. Pin. Sur un cas particulier de la conjecture de Cerny. In *Automata, languages and programming (Fifth Internat. Colloq., Udine, 1978)*, volume 62 of *Lecture Notes in Comput. Sci.*, pages 345–352. Springer, Berlin, 1978.
17. J.-E. Pin. Le problème de la synchronisation et la conjecture de Černý. In *Noncommutative structures in algebra and geometric combinatorics (Naples, 1978)*, volume 109 of *Quad. “Ricerca Sci.”*, pages 37–48. CNR, Rome, 1981.
18. J.-E. Pin. On two combinatorial problems arising from automata theory. In *Combinatorial mathematics (Marseille-Luminy, 1981)*, volume 75 of *North-Holland Math. Stud.*, pages 535–548. North-Holland, Amsterdam, 1983.
19. I. Rystsov. Reset words for commutative and solvable automata. *Theoret. Comput. Sci.*, 172(1-2):273–279, 1997.
20. I. C. Rystsov. On the rank of a finite automaton. *Kibernet. Sistem. Anal.*, (3):3–10, 187, 1992.
21. I. K. Rystsov. Quasioptimal bound for the length of reset words for regular automata. *Acta Cybernet.*, 12(2):145–152, 1995.
22. I. K. Rystsov. On the length of reset words for automata with simple idempotents. *Kibernet. Sistem. Anal.*, (3):32–39, 187, 2000.

23. A. Salomaa. Composition sequences for functions over a finite domain. *Theoret. Comput. Sci.*, 292(1):263–281, 2003. Selected papers in honor of Jean Berstel.
24. B. Steinberg. The averaging trick and the Černý conjecture, October 2009. <http://arxiv.org/abs/0910.0410>.
25. B. Steinberg. Černý’s conjecture and group representation theory. *J. Algebr. Comb.*, 31(1):83–109, 2010.
26. A. N. Trahtman. An efficient algorithm finds noticeable trends and examples concerning the Černý conjecture. In *Mathematical foundations of computer science 2006*, volume 4162 of *Lecture Notes in Comput. Sci.*, pages 789–800. Springer, Berlin, 2006.
27. A. N. Trahtman. The Černý conjecture for aperiodic automata. *Discrete Math. Theor. Comput. Sci.*, 9(2):3–10 (electronic), 2007.
28. A. N. Trahtman. The road coloring problem. *Israel J. Math.*, 172:51–60, 2009.
29. J. Černý. A remark on homogeneous experiments with finite automata. *Mat.-Fyz. Časopis Sloven. Akad. Vied*, 14:208–216, 1964.
30. M. V. Volkov. Synchronizing automata and the Černý conjecture. In C. Martín-Vide, F. Otto, and H. Fernau, editors, *Language and Automata Theory and Applications Second International Conference, LATA 2008, Tarragona, Spain, March 13-19, 2008.*, volume 5196 of *Lecture Notes in Computer Science*, pages 11–27, Berlin / Heidelberg, 2008. Springer.